Security in IoT-Driven Mobile Edge Computing: New Paradigms, Challenges, and Opportunities

Sahil Garg, Member, IEEE, Kuljeet Kaur, Member, IEEE, Georges Kaddoum, Member, IEEE, Prasad Garigipati, and Gagangeet Singh Aujla, Senior Member, IEEE

***Abstract*—With the exponential growth in the number of connected devices, recent years have seen a paradigm shift towards mobile edge computing. As a promising edge technology, it pushes mobile computing, network control, and storage to the network edges so as to provide better support to computation-intensive Internet of Things (IoT) applications. Although it enables offloading latency-sensitive applications at the resource-limited mobile devices, decentralized architectures and diversified deployment environments bring new security and privacy challenges. This is due to the fact that, with wireless communications, the medium can be accessed by both legitimate users and adversaries. Though cloud computing has helped in substantial transformation of the global business, it falls short in provisioning distributed services, namely, security of IoT systems. Thus, the ever-evolving IoT applications require robust cyber-security measures particularly at the network's edge, for widespread adoption of IoT applications. In this vein, the classical machine learning models devised during the last decade, fall short in terms of low accuracy and reduced scalability for real-time attack detection across widely dispersed edge nodes. Thus, the advances in areas of deep learning, federated learning, and transfer learning could mark the evolution of more sophisticated models that can detect cyberattacks in heterogeneous IoT-driven edge networks without human intervention. We provide a SecEdge-Learn Architecture that uses deep learning and transfer learning approaches to provided a secure MEC environment. Moreover, we utilised blockchain to store the knowledge gained from the MEC clusters and thereby realising the transfer learning approach to utilise the knowledge for handling different attack scenarios. Finally, we discuss the Industry relevance of the MEC environment.**

***Index Terms*—Mobile Edge Computing, Cloud Computing, Internet of Things, 5G, Cyber-security, Deep learning, Reinforcement learning, Time-series analysis, and Quality of Experience.**

I. Introduction

With the rapid advancements in wireless networks, mobile operators have been witnessing an astonishing increase in mobile data traffic. While providing a remarkable improvement to the quality of lives, exponential growth of mobile terminals is foreseen to impose an unprecedented pressure on the backbone network, triggering challenges for cellular and wireless networks. In addition, the emerging IoT technology is expected to further stumble these networks, resulting in an explosive growth of Global Internet users. According to Cisco Visual Networking Index, 27.1 billion networked devices and connections will be used by 2022, contributing to a global Internet traffic of 4.8 ZB comparable to 1.5 ZB in 2017 [1]. Moreover, the thriving demand of computational intensive applications has gained momentous ground to alleviate resource deficiencies of mobile devices (e.g. lower processing power, limited memory capacity, and constrained battery life).

The IoT infrastructure has been largely impacted by the evolution of different network technologies (from 1G to 5G). However, this gradual evolution, IoT has embarked a universal stature and developed different forms, namely massive IoT, broadband IoT, Commercial IoT, and Industrial automation IoT. The related details are highlighted in the Fig. 1. These developments are clearly indicative from the increasing penetration of Internet users and connected devices. Consequently, Gartner believes that the global IoT market will grow upto 19 Trillion by 2020 [2]. In spite of all the advancements in recent years, smart mobile devices are still low potential computing devices; constrained by their miniature size, weight, storage capacity, and intrinsic limitations w.r.t wireless medium and mobility. Such soaring demands for data services with immersive Quality of Experience (QoE) are gaining ground towards higher network and computation requirements.

In the past decade, mobile cloud computing (MCC) has gained popularity, where a resource-rich cloud is used as a platform to execute resource-intensive mobile applications. By integrating mobile computing and cloud computing, MCC provided considerable capabilities to mobile devices and empowered them with computing, storage, and energy resources to enrich the computing experience of mobile users [3]. Through MCC technology, mobile devices can continuously offload the computing power and data storage requirements on powerful centralized computing data centers that could not otherwise be supported. As of today, multiple services are available for augmenting storage potentials of mobile devices, such as Dropbox, Amazon S3, iCloud, Google Drive, MobileMe, and Skydrive. However, safety and reliability issues brought by third party's cloud systems have been the major challenges for users utilizing such services. Moreover, the emerging trend of IoT deployment pose new requirements in front of MCC, such as geo-distribution support, real-time response, mobility support, low-latency, and location awareness. However, traditional cloud setting cannot satisfy these demands for a wide-range of emerging mobile applications due to longer response times, affecting the QoE for end users. Thus, large-scale IoT deployments suggest the urgent need for a distributed

S. Garg, K. Kaur, and G. Kaddoum are with the Electrical Engineering Department, École de technologie supérieure, Université du Québec, Montréal, QC H3C 1K3, Canada (e-mail: sahil.garg@ieee.org, kuljeet.kaur@ieee.org, and georges.kaddoum@etsmtl.ca)

P. Garigipati is with the Global AI Accelerator at Ericsson, Montreal, Canada (e-mail: prasad.garigipati@ericsson.com)

G.S. Aujla is with the Department of Computer Science, Durham University, Durham, UK (e-mail: gagi_aujla82@yahoo.com)

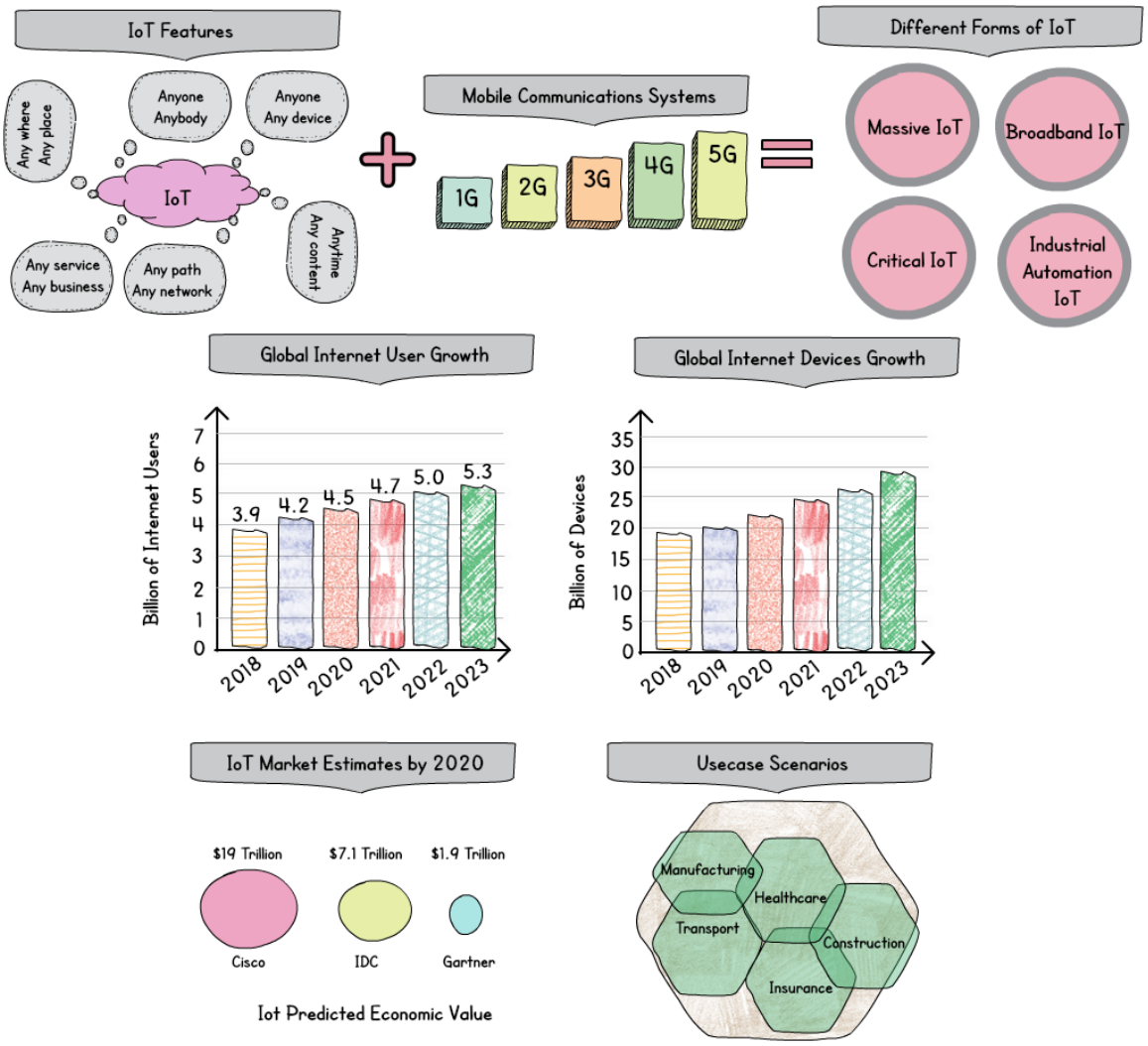

Fig. 1: Evolution of different network technologies

computing platform that can support the interactions between IoT and cloud computing systems [4].

Driven by the visions of IoT and 5G communications, a new trend in computing has emerged that extend the cloud and its services to the edge of the network. This paradigm is called Mobile Edge Computing (MEC) - a step further on the MCC [5]. By pushing data intensive tasks towards the edge, it offers several advantages, such as location awareness, real-time response, high mobility support, low bandwidth requirements, high throughput, and low latency, all due to its proximity to terminal devices. It also offers an open radio network edge platform in order to facilitate the use of the storage and processing capabilities. Therefore, the MEC has a wide range of applications, such as healthcare, connected vehicles, video analytics, virtual reality, smart communities, mobile big data analytics, smart grid, etc.

Broadly the paradigm of Edge Computing can be segregated into four main types, i.e. device/mobile edge, on-premise edge, telecom edge, and centralized cloud edge. These are shown clearly using Fig. 2. The edge computing infrastructure is largely supported by different mobile devices such as laptops, mobiles, smart watches, smart camera, smart cars, etc. These devices help to provide immediate and seamless services at the edge of the network. However, with gradual advances in technologies, many companies have also invested in different forms of on-premise edge computing facilities which support co-location and sharing of resources. On the other hand, there is the first layer of edge computing that is supported by the telecom industry and referred to as the telecom edge. It offers strict realtime services with high performance index. And finally, the largest and the most powerful of all is the cloud edge that has fairly abundant resources but distantly located.
Though MEC has been envisioned as an enabling technology to support local IoT applications, it faces a variety of security and privacy threats. On one hand, it inherits security issues from cloud computing whereas, on the other hand, decentralized architectures and diversified deployment environments raise the security consciousness to the next level. So, it is important to develop security and privacy-preserving solutions for MEC to support computing-based IoT applications and open a wider market for application developers.

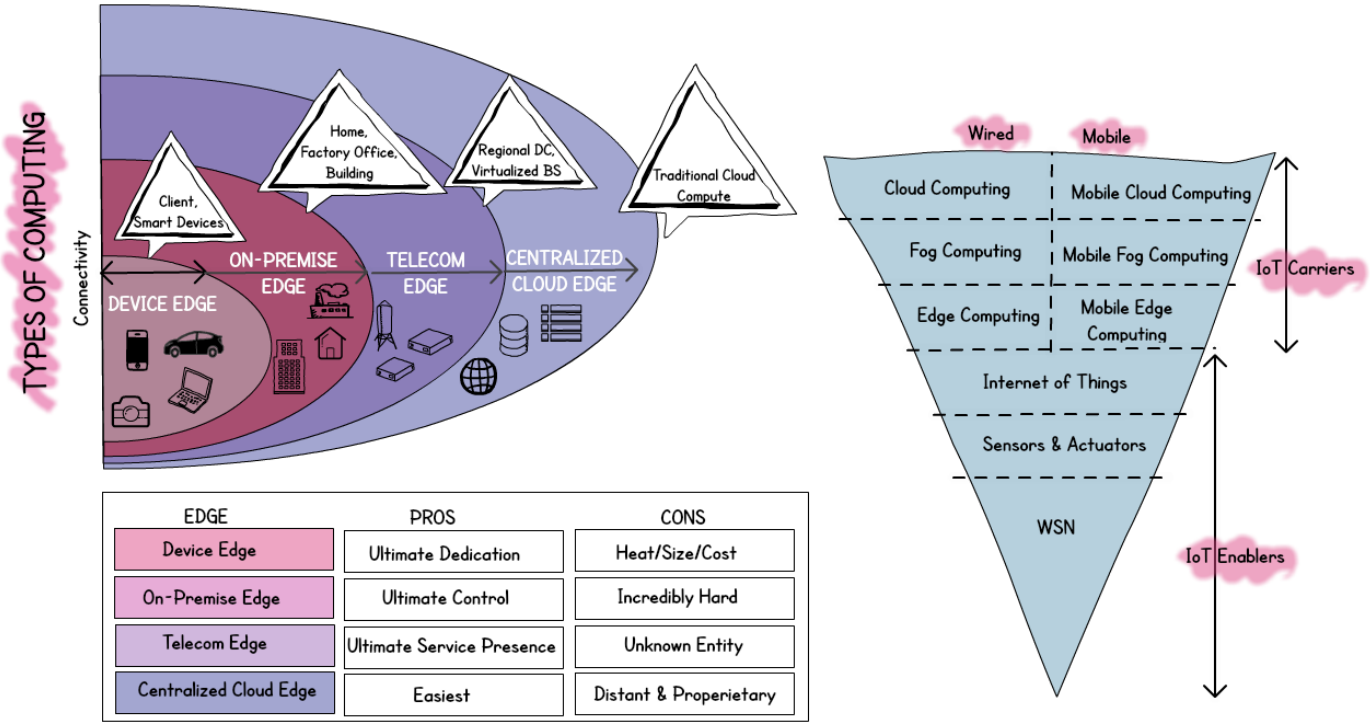

Fig. 2: Overview of Edge Computing Framework

TABLE I: Comparative analysis of the existing schemes.

Work	Environment	Technique Used	Scope
Du *et. al* [6]	MEC	Machine Learning	Privacy preservation during data aggregation
Xiao *et. al* [7]	MEC	A collaborative security mechanism based on reinforcement learning, authentication, and secure caching scheme	Security against data offloading and higher data privacy
Chen *et. al* in [8]	MEC	DL model to order to learn the attack features using unsupervised learning	Communication security
He *et. al* [9]	MSNs	A social trust scheme based on a deep reinforcement model	For enhanced security and efficiency of networks
Diro and Chilamkurti [10]	Fog-to-thing computing	DL	For cyber-threat detection
Dai *et. al* in [11]	IoT	AI and Blockchain	Improved flexibility and security of wireless networks
Khelifi *et. al* [12]	IoT-based MECs	Different DL models	Data processing and analysis
Wang *et. al* [13]	MEC	Integration of deep reinforcement learning and federated learning	Improved caching mechanism
Lu *et. al* [14]	Distributed edge computing in vehicular networks	Federated learning	Enhanced security

II. Literature Review

MEC is essentially employed to perform the compute-intensive applications at the edge of transportation-driven networks. However, over the course of time, the associated traffic has seen prolific growth. Subsequently, security of the underlying networks has become a mainstream concern for the research community. Thus, in this direction, several proposals have been proposed in the literature. Some of the notable contributions are depicted in Table I and described below.

The authors in [6] devised a privacy persevering scheme based on machine learning, particular for data aggregation and data mining in MEC setups. According to the authors, the MEC environments are easily prone to security attacks due to the lack of a centralized management system for managing the distributed mobile edge nodes. Once a single node is hijacked by the attacker, the cyber attacks can easily propagate across the network. Thus, the authors proposed a novel architecture for MEC in heterogeneous IoT scenario. Likewise, Xiao *et. al* [7] investigated in detail the attack models in MEC environments. More importantly, the authors also proposed a collaborative security mechanism based on reinforcement learning, authentication, and secure caching scheme. The former was employed for security against data offloading onto the edge nodes, particularly against jamming threats. On the contrary, the latter two were used for higher data privacy. In a similar direction, Chen *et. al* in [8] identified the problem of communications security in the MEC environments. Consequently, the authors designed a deep learning (DL) model to order to learn the attack features from the heterogeneous MEC setup using active unsupervised learning approach.

In [9], authors focused on the security aspect of the Mobile

social networks (MSNs), a variant of MEC. The authors believed the information about social relationships amongst the users is an important perquisite to enhance the security and efficiency of these networks. Thus, they proposed a social trust scheme based on a deep reinforcement model; wherein the model automatically executes for optimal resource allocations. Likewise, Diro and Chilamkurti [10] devised a cyber-threat detection scheme based on the concepts of DL in the context to fog-to-things computing. Dai *et. al* in [11] identified the Blockchain and AI as the next most powerful technologies for the wireless networks. In this context, the authors propounded the integration of Blockchain and AI to improve the performance of the wireless networks in terms of flexibility and security. In detail, the content caching scheme was designed by the authors using both blockchain and deep reinforcement learning.

In IoT-driven MEC setups, data processing and analysis is a daunting task. In this context, efficient models based of DL and transfer learning (TL) can play a pivotal role. This is because majority of the data in IoT-based MECs is essentially device-driven; wherein manual interferences are not required for data receiving and processing [12]. Thus, authors in [12] merged different machine learning models based on DL with the IoT's information-centric networking deployed at the edge of the network. In [13], Wang *et. al* proposed the integration of deep reinforcement learning and federated learning for enhancing the performance of MEC's caching and communication. The authors referred to this framework as the "In-Edge AI" and it leveraged the benefits of both the devices and edge nodes for exchanging the learning parameters in real-time for high accuracy inferences. Lu *et. al* [14] identified federated learning as a promising technology for distributed edge computing; wherein the edge nodes can locally train their respective models with the need to transmit their data to the central sever. Nonetheless, the approach is novel but is prone to security and privacy issues.

III. Motivation and Contributions

While applications of the heterogeneous IoT proliferate, the data security and privacy protection mechanisms of the cloud computing environment are no longer applicable to MEC deployments. This creates a strong need to protect the data from potential security threats ranging from privacy breaches to network availability and critical information misuse. However, the increasingly connected technological landscape raises significant challenges to the current MEC paradigm. This includes access control, heterogeneity of MEC systems, identity authentication, privacy preservation, secure data aggregation, mis-configurations, diversity of communication technologies, secure content distribution, resilience to attacks, lightweight protocol design, establishing trustworthy data sharing practices, etc [15]. In addition, the lack of comprehensive security mechanism render the deployment of MEC a technically challenging problem. Further, the security goals of MEC—confidentiality, integrity, availability, safety, and resiliency—should be grounded on a combined objective of securing the data and ensuring the safety and resiliency of systems and processes. Thus, we aim to secure the distributed applications and services for MEC through layered security models wherein an effective hierarchical mechanism will be developed in order to maintain a more secure and resilient operating environment. However, the classical machine leaning models fall short in terms of low accuracy and reduced scalability for real-time attack detection across widely dispersed edge nodes. Thus, the advances in areas of DL could mark the evolution of more sophisticated models that can detect cyberattacks in heterogeneous IoT-driven edge networks without human intervention.

IV. Proposed Paradigm: SecEdge-Learn

The proposed architecture of the secure MEC ecosystem based on different learning mechanisms is described comprehensively in the subsequent sections.

A. System Model

The proposed system model of the secure MEC environment is shown in Fig. 3. The overall architecture can be segregated into the following three layers, namely, mobile devices, MEC servers, and the Internet core layer. The lowest layer comprises of the mobile nodes at the edge of the network. These devices are connected with the MEC servers via a high speed link. The MEC servers are comparatively more powerful than the mobile devices and provide the required services with reduced latency. They are geographically distributed and form the core of the MEC environment. This layer is connected to the upper most layer via the backbone network. The uppermost layer comprises of the computation intensive data centers.

An attacker in the MEC environment can launch attack at various layers in the form of an adversary at the middle layers or as a jammer or rogue mobile device at the lowest layer. The different attack vectors that can be exploited by the attacker fall in the range of man-in-the-middle attack, jamming attack, denial of service attack, spoofing attack, etc.

B. Proposed Scheme

Thus, in order to safegaurd the MEC environment, a DL model can be leveraged that comprises of different stages (as shown in Fig. 3) such as:-

- *Data acquisition*: In particular, a set of features from the MEC environment is used as the unlabeled samples which are used to analyze attack behaviors
- *Preprocessing and Feature extraction*: The feature extraction module uses static/dynamic learning to preprocess the attack features.
- *Classification*: This phase (also known as detection module) uses this knowledge to make the attack detections.

Recent neural network models trained on large data sets can obtain impressive performance across a wide variety of IoT domains. But training these neural network models is an expensive task especially for multivariate time-series data. Unlike regression predictive modeling, time series adds the complexity of a sequence dependence among the input variables. In this direction, a long short-term memory (LSTM)

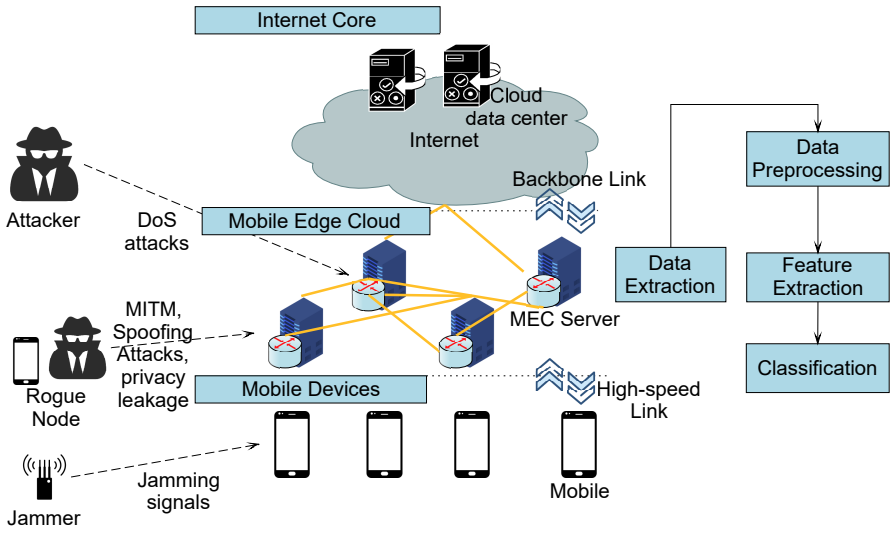

Fig. 3: Secure three-layer MEC Architecture

neural network is considered as one of the powerful tool to find the patterns of time sequential data. Thus, we propose a LSTM model in order to achieve an optimal level of security with reduced computational overhead. Further, reinforcement learning (RL) has been proven to excel in sequential decision-making tasks. One of the key features of RL is the focus on learning a control policy to optimize the choice of actions over several time steps. In lieu of this, the proposed scheme is devised to operate in two phases: prediction and detection.

- In the first phase, prediction phase, a LSTM-based neural network is trained by investigating the features and patterns of MEC time-series data.
- In the second phase, attack detection, we employ RL approach to detect attacks using the trained model.

The above approach is suitable for application in a limited scenario where only a single MEC cluster is deployed. However, when we have multiple MEC clusters, then we need an approach that supports the cluster-wide distribution by utilising the experience based on the above two phases in a single cluster. For this reason, we can use TL that supports storing of the knowledge gained form one MEC cluster and using it for a different attack scenario in another MEC cluster. Let us consider a case study to provide more clarity. In Fig. 4, we have shown different MEC clusters serving different applications (such as mobile clients, vehicle clients, smart home clients) at the same time. Now, if an attacker injects a malicious script in the MEC cluster 1 using a compromised mobile client, then our DL approach will help us to predict and detect the attack in the MEC cluster using the two steps based on LSTM and RL approaches. However, if another attacker targets a different MEC cluster (let us say cluster 2) in the future, then we have to repeat the same process again without improvising the DL model using the attack scenario handled in MEC cluster 1. One way to resolve this problem is to perform the computationally expensive process of training the model again but this can lead to inconsistencies, add to the complexity, and generate additional overheads. So to resolve this problem, we used the TL approach that helps us to transfer the learning gained in the cluster 1 to other clusters. This way we can improve the efficiency of the RL Agent (Smart Agent in Fig. 4) significantly. To realise this TL approach in MEC environment, we store the activity log of each cluster, that can be used by the Smart Agents to transfer the knowledge gained in different clusters to make it cluster-wide distribution. However, there may be a chance of redundancy of same knowledge being stored in the logs. So, to resolve this issue, we deployed a blockchain network to validate each activity log before using it for TL process. Once validated, it can be distributed cluster-wide for further TL tasks. So, this means we have two additional phases, depicted as below.

- In the third phase, blockchain phase, the activity log collected from the above two phases is added to the ledger and approved for a cluster wide distribution. The steps followed in this phase are,
  - A Smart Agent (also known as Learn Engine) is deployed in each MEC cluster that is responsible for all the tasks related to the learning mechanism. The attack prediction and detection data is added to the activity log and this log is added to a unique block with the cluster identifier.
  - It is then verified though a blockchain network and and added to the ledger.
  - On verification, the activity log is approved for cluster-wide utilisation by Smart Agents through TL approach. In case a similar log is already available in the blockchain, it is not added to the blockchain.
- In the fourth phase, a TL approach is used to extract the knowledge gained from other clusters and stored in the ledger and thereafter use the same to handle different attack scenarios through the MEC environment.

The workflow of the proposed SecEdge-Learn scheme is presented using a sequence diagram as shown in Fig. 5

V. Open Issues and Challenges

To realise the above proposed architecture, there are several research challenges and open issues that need to be addressed.

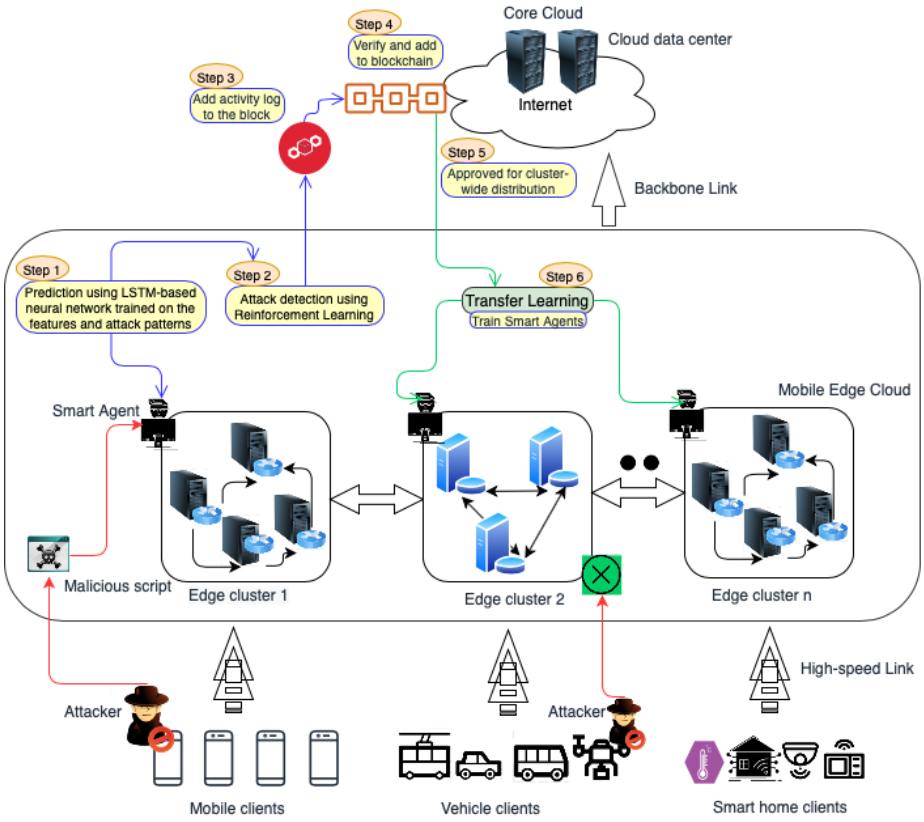

Fig. 4: An illustration of the proposed SecEdge-Learn Architecture

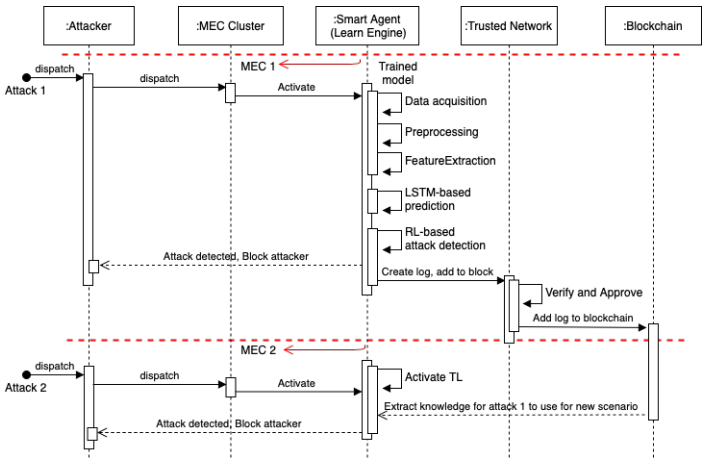

Fig. 5: Sequence of activities in SecEdge-Learn

Some of them are listed below:

- *Lack of provision of Policy Enforcement:* There is significant impact of the lack of uniform policy enforcement functions like, IP whitelisting, Virtual LAN, and VPN termination that can lead towards issues related to the integrity of the MEC network
- *Age of Data:* The data freshness is one of the key factors for the success of critical applications running in the MEC environment. Even more, the proposed learning architecture has the tendency towards the degradation of efficiency due the age of data (specifically for TL).
- *Edge-cloud Coordination:* The lack of reliable cloud-edge communication capabilities to handle the processing instances related to cloud services requiring real-time support can lead to drastic performance issues.
- *Secure Interworking among Networks/Clusters:* As one MEC network has to interwork with another network (for example, a carrier's MEC network has to coordinate with an enterprise to ensure the provision of 5G capabilities), the reliance on the MEC routers can lead to security challenges and requires a firewall-based network solution.
- *MEC-Blockchain Synergy:* The coordination of MEC and blockchain has not been deeply looked across in industrial deployments, so there are several hidden challenges that may come across for practical deployments.
- *Complexity and Overheads:* The deployment of multiple learning mechanisms can in itself lead to challenging scenarios where it can be tough to maintain the overheads and sustain the complexity.
- *Transition from 5G to 6G:* The adoption of 5G and transition towards 6G can lead to unexpected challenges (interconnections and interfaces, coordination, user plane function, management and control, and interworking between mobile and fixed bearers) for carrier access network in large scale MEC deployments.
- *Safety of Metadata or Sensitive Data:* The risk of the loss of data (sensitive or meta data) related to the organisation or business enterprise activity and browsing behaviour

can end up in serious implications from hackers using compromised edge devices.

VI. Directions and Opportunities Relevant to the Industry

With the proliferation of IoT, existing and upcoming next-generation technologies such as software-defined networking, autonomous vehicles (AUVs), augmented/virtual reality, and industrial automation are fueling innovations across several industries. As the size of IoT systems grow to large scale, their impact will also increase on enterprise systems and consumer's everyday lives. Thus, enabling applications to make near real-time decisions will be required in order to pave the way for enhanced QoE and securing greater demand for services. When paired with 5G, which promises improved capacity, high bandwidth, and lower latency, MEC will create faster, more efficient and intelligent networks while unlocking new possibilities for digital businesses. Apart from hosting new 5G services, the other major network operator driver for MEC is deploying virtualized network infrastructure, which in turn is a key enabler for providing dynamic network slicing vital for 5G services. By shifting resources to the edge, MEC will enable new scenarios such as: augmented reality, mass IoT, robotics, AUVs/drones, etc and it is foreseen that the influence of these next generation systems will probably be available by the end of 2020. According to Gartner, "75% of enterprise data will be processed outside traditional data centers or cloud by 2022 which is 10% till date" [2]. Enterprises are deriving benefits from MEC in the form of more efficient utilization of network capacity. But as more rich media and time-critical applications are deployed to benefit from this wireless network, security vulnerabilities are bound to increase. And as the network becomes more connected, security breaches can be contagious. Thus, to sustain their capacity and maintaining QoE to subscribers, it is important to navigate through the opportunities and challenges of edge intelligence. In this direction, integrating DL models into edge devices will reduce the strain on overburdened networks and protects essential services from outages or dependency issues. As a whole, this technology is poised to provide ample opportunities for businesses with a high potential for growth.

VII. Conclusion

The massive deployment of IoT applications across every vertical of the global development has pushed the computing and storage to edge of the network. MEC paradigm has the capability to offload the real-time applications in the local domain (closer to the user) at the compute-limited mobile devices. However, the open access and communication medium opens this paradigm to adversaries and attackers. Due to this backdrop, we have investigated various security and privacy challenges for MEC deployment in diverse application domains. Furthermore, we utilised the learning technologies (DL and TL) to suggest a potential security architecture for MEC environment that has the capability to understand the patterns of data or actions originating from different layers and thereafter using these patterns to detect the potential attacks or threat within a stipulated time. The potential challenges and open issues that can impact the proposed security paradigm are also discussed. Finally, the relevance and opportunities relevant to the industry concerning the secure MEC deployment are also discussed. As a future prospective, we eye towards realising a practical prototype of the proposed secure MEC paradigm using different learning technologies relevant to different industrial applications.

Acknowledgement

This work was supported by the Ericsson's Global Artificial Intelligence Accelerator (GAIA), Montreal, Canada through MITACS Accelerate program and also by the Fonds de recherche du Québec – Nature et technologies (FRQNT) through PBEEE via File No. 287201.

References

[1] (2018) Cisco Visual Networking Index: Forecast and Trends, 2017–2022. Cisco. [Accessed on: Jan. 2020]. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf

[2] (2018) 5G Edge Computing Whitepaper. Federal Communications Commission. [Accessed on: Jan. 2020]. [Online]. Available: https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/20 18/5G-Edge-Computing-Whitepaper-v6-Final.pdf

[3] M. Shiraz, A. Gani, R. H. Khokhar, and R. Buyya, "A Review on Distributed Application Processing Frameworks in Smart Mobile Devices for Mobile Cloud Computing," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 1294–1313, 2013.

[4] S. Wang, Y. Guo, N. Zhang, P. Yang, A. Zhou, and X. S. Shen, "Delay-aware microservice coordination in mobile edge computing: A reinforcement learning approach," *IEEE Transactions on Mobile Computing*, 2019, DOI: 10.1109/TMC.2019.2957804.

[5] T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, "Collaborative Mobile Edge Computing in 5G Networks: New Paradigms, Scenarios, and Challenges," *IEEE Communications Magazine*, vol. 55, no. 4, pp. 54–61, 2017.

[6] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, "Big data privacy preserving in multi-access edge computing for heterogeneous internet of things," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 62–67, 2018.

[7] L. Xiao, X. Wan, C. Dai, X. Du, X. Chen, and M. Guizani, "Security in mobile edge caching with reinforcement learning," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 116–122, 2018.

[8] Y. Chen, Y. Zhang, S. Maharjan, M. Alam, and T. Wu, "Deep learning for secure mobile edge computing in cyber-physical transportation systems," *IEEE Network*, vol. 33, no. 4, pp. 36–41, 2019.

[9] Y. He, F. R. Yu, N. Zhao, and H. Yin, "Secure social networks in 5g systems with mobile edge computing, caching, and device-to-device communications," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 103–109, 2018.

[10] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog-to-things computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, 2018.

[11] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond," *IEEE Network*, vol. 33, no. 3, pp. 10–17, 2019.

[12] H. Khelifi, S. Luo, B. Nour, A. Sellami, H. Moungla, S. H. Ahmed, and M. Guizani, "Bringing deep learning at the edge of information-centric internet of things," *IEEE Communications Letters*, vol. 23, no. 1, pp. 52–55, 2018.

[13] X. Wang, Y. Han, C. Wang, Q. Zhao, X. Chen, and M. Chen, "In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning," *IEEE Network*, vol. 33, no. 5, pp. 156–165, 2019.

[14] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Differentially private asynchronous federated learning for mobile edge computing in urban informatics," *IEEE Transactions on Industrial Informatics*, 2019.

[15] A. Alnoman, G. H. S. Carvalho, A. Anpalagan, and I. Woungang, "Energy Efficiency on Fully Cloudified Mobile Networks: Survey, Challenges, and Open Issues," *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 1271–1291, 2018.